WHAT IS CLAIMED IS:

1. A system for secure communication, comprising:

a random value generator configured to generate a random value;

a message validation code generator coupled to the random value generator and configured to generate a message validation code based on a predetermined key, a message, and the random value;

a one-time pad generator coupled to the random number generator and configured to generate a one-time pad based on the random value and the predetermined key; and

a masked message generator coupled to the one-time pad generator and configured to generate a masked message based on the one-time pad and the message.

2. The system as recited in claim 1, wherein the message validation code generator employs a first one-way hash function.

3. The system as recited in claim 2, wherein the one-time pad generator employs the first one-way hash function.

4. The system as recited in claim 1, wherein the message validation code generator employs a first one-way hash function and the one-time pad generator employs a second one-way hash function.

5. The system as recited in claim 1, further comprising a protected message envelope generator coupled to the random value generator, the message validation code generator, and the masked message generator, and configured to generate a protected message envelope based on the random value, the message validation code, and the masked message.

6. The system as recited in claim 5, further comprising a transmitter coupled to the protected message envelope generator and configured to transmit the protected message envelope to a target.

7. A system for secure communication, comprising:

a protected message envelope reader configured to receive a protected message envelope and generate a random value, a masked message, and a first message validation code based on the received protected message envelope;

a one-time pad generator coupled to the protected message envelope reader and configured to generate a one-time pad based on the random value and a predetermined key; and

a message unmasker coupled to the one-time pad generator and protected message envelope reader, and configured to generate an unmasked message based on the one-time pad and the masked message.

8. The system as recited in claim 7, wherein the one-time pad generator employs a first one-way hash function.

9. The system as recited in claim 7, further comprising a validation module coupled to the protected message envelope reader and the message unmasker, the validation module comprising:

a message validation code generator configured to generate a second message validation code based on the predetermined key, the unmasked message, and the random value; and

a message validation code comparator coupled to the protected message envelope reader and the message validation code generator and configured to generate a validation based

on the first message validation code and the second message validation code.

10. The system as recited in claim 9, wherein the validation module employs a first one-way hash function.

11. The system as recited in claim 9, wherein the validation module employs a first one-way hash function and the one-time pad generator employs a second one-way hash function.

12. A method for secure communication, comprising:

generating a random value;

generating a message validation code based on a message, the random value, a predetermined key, and a first one-way hash function;

generating a one-time pad based on the random value, the predetermined key, and a second one-way hash function; and

generating a masked message based on the message and the one-time pad.

13. The method as recited in claim 12, further comprising generating a protected message envelope based on the random value, the masked message, and the message validation code.

14. The method as recited in claim 13, further comprising transmitting the protected message envelope to a target destination.

15. The method as recited in claim 12, wherein the first one-way hash function and the second one-way hash

function are the same one-way hash function.

16. A secure message generated by the method of claim 12.

17. A secure message generated by the method of claim 13.

18. A method for secure communication, comprising:

receiving a random value, a masked message, and a first message validation code;

generating a one-time pad based on the random value, a predetermined key, and a first one-way hash function; and

generating an unmasked message based on the one-time pad and the masked message.

19. The method as recited in claim 18, further comprising:

generating a second message validation code based on the unmasked message, the random value, the predetermined key and a second one-way hash function; and

comparing the first message validation code to the second message validation code to determine a validity of the unmasked message.

20. The method as recited in claim 19, wherein the first one-way hash function and the second one-way hash function are the same one-way hash function.

21. The system of claim 18, further comprising:

receiving a protected message envelope; and

generating a random value, a masked message, and a first message validation code based on the received

protected message envelope.

22. A computer program product for secure communications, the computer program product having a medium with a computer program embedded thereon, the computer program comprising:

computer code for generating a random value;

computer code for generating a message validation code based on a message to be sent, the random value, a predetermined key, and a first one-way hash function;

computer code for generating a one-time pad based on the random value, the predetermined key, and a second one-way hash function;

computer code for generating a masked message based on the message to be sent and the one-time pad; and

computer code for generating a protected message envelope based on the random value, the masked message, and the message validation code.

23. A computer program product for secure communications, the computer program product having a medium with a computer program embedded thereon, the computer program comprising:

computer code for receiving a protected message envelope;

computer code for generating a random value, a masked message, and a first message validation code based on the protected message envelope;

computer code for generating a one-time pad based on the random value, a predetermined key, and a first one-way hash function;

computer code for generating an unmasked message based on the one-time pad and the masked message;

computer code for generating a second message validation code based on the unmasked message, the random value, the predetermined key, and a second one-way hash function; and

computer code for comparing the first message validation code to the second message validation code to determine a validity of the unmasked message.